

IN THE CLAIMS

What is claimed is:

1. 1. A computer software product including one or more recordable media having executable instructions stored thereon which, when executed by a processing device, causes the processing device to:
  4. initialize a symbolic simulation relation for an assertion graph on a first symbolic lattice domain.
1. 2. The computer software product recited in Claim 1 wherein initializing the symbolic simulation relation comprises causing the processing device to:
  3. join a Boolean predicate for an outgoing edge from an initial vertex in the assertion graph with a symbolic antecedent labeling of an edge in the assertion graph.
1. 3. The computer software product recited in Claim 2 wherein the symbolic antecedent labeling comprises a symbolic indexing function to encode a plurality of antecedent labels for a plurality of assertion graph instances, having at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.
1. 4. The computer software product recited in Claim 1 wherein the assertion graph on the first symbolic lattice domain is configurable to express a justification property to verify by computing the symbolic simulation relation.
1. 5. The computer software product recited in Claim 4 which, when executed by a processing device, further causes the processing device to:
  3. compute the symbolic simulation relation for the assertion graph on the first symbolic lattice domain; and
  5. check the symbolic simulation relation to verify a plurality of properties

6 expressed by a plurality of assertion graph instances, having at least one  
7 assertion graph instance on a second lattice domain different from the first  
8 symbolic lattice domain.

- 1 6. The computer software product recited in Claim 1 which, when executed by a  
2 processing device, further causes the processing device to:

3 compute the symbolic simulation relation for the assertion graph on the  
4 first symbolic lattice domain; and

5 compare the symbolic simulation relation to a symbolic consequence  
6 labeling for the edge for the assertion graph on the first symbolic lattice  
7 domain.

- 1 7. The computer software product recited in Claim 6 wherein computing the  
2 symbolic simulation relation comprises causing the processing device to:

3 join the symbolic simulation relation for the assertion graph on the first  
4 symbolic lattice domain, to any states that are contained by a symbolic  
5 antecedent for a first plurality of edges of the assertion graph on the first  
6 symbolic lattice domain and also contained by a symbolic post-image for a  
7 second plurality of edges incoming to the first plurality of edges.

- 1 8. The computer software product recited in Claim 1 which, when executed by a  
2 processing device, further causes the processing device to:

3 compute the symbolic simulation relation for the assertion graph on the  
4 first symbolic lattice domain to verify the assertion graph according to a  
5 normal satisfiability criteria.

- 1 9. A method comprising:

2 initializing a symbolic simulation relation for an assertion graph on a first  
3 symbolic lattice domain.

- 1    10. The method recited in Claim 9 wherein initializing the symbolic simulation  
2       relation comprises:  
3           joining a Boolean predicate for an outgoing edge from an initial vertex in  
4       the assertion graph with a symbolic antecedent labeling of an edge in the  
5       assertion graph.
- 1    11. The method recited in Claim 10 wherein the symbolic antecedent labeling  
2       comprises a symbolic indexing function to encode a plurality of antecedent  
3       labels for a plurality of assertion graph instances, having at least one  
4       assertion graph instance on a second lattice domain different from the first  
5       symbolic lattice domain.
- 1    12. The method recited in Claim 9 further comprising:  
2           computing the symbolic simulation relation for the assertion graph on the  
3       first symbolic lattice domain; and  
4           comparing the symbolic simulation relation to a symbolic consequence  
5       labeling for the edge for the assertion graph on the first symbolic lattice  
6       domain.
- 1    13. The method recited in Claim 12 wherein computing the symbolic simulation  
2       relation comprises:  
3           joining the symbolic simulation relation for the assertion graph on the first  
4       symbolic lattice domain, to any states that are contained by a symbolic  
5       antecedent for a first plurality of edges of the assertion graph on the first  
6       symbolic lattice domain and also contained by a symbolic post-image for a  
7       second plurality of edges incoming to the first plurality of edges.
- 1    14. The method recited in Claim 9 wherein the assertion graph on the first  
2       symbolic lattice domain is configurable to express a justification property to  
3       verify through computing the symbolic simulation relation.

- 1    15. The method recited in Claim 14 further comprising:
- 2                computing the symbolic simulation relation for the assertion graph on the
- 3                first symbolic lattice domain; and
- 4                checking the symbolic simulation relation to verify a plurality of properties
- 5                expressed by a plurality of corresponding assertion graph instances, having
- 6                at least one assertion graph instance on a second lattice domain different
- 7                from the first symbolic lattice domain.
- 1    16. A method comprising:
- 2                specifying a justification property with an assertion graph.
- 1    17. The method recited in Claim 16 wherein the assertion graph is on a first
- 2                symbolic lattice domain; and the justification property is expressed by one of
- 3                a plurality of instances of the assertion graph, at least one assertion graph
- 4                instance on a second lattice domain different from the first symbolic lattice
- 5                domain.
- 1    18. The method recited in Claim 17 further comprising:
- 2                computing a symbolic simulation relation for the assertion graph on the
- 3                first symbolic lattice domain; and
- 4                checking the symbolic simulation relation with a symbolic consequence
- 5                labeling for the assertion graph on the first symbolic lattice domain according
- 6                to a normal satisfiability criteria.
- 1    19. A method comprising:
- 2                merging a plurality of properties in an assertion graph on a first symbolic
- 3                lattice domain by using a symbolic labeling.
- 1    20. The method recited in Claim 19 wherein the symbolic labeling comprises a
- 2                symbolic indexing function to encode a plurality of labels for a plurality of

3 assertion graph instances, having at least one assertion graph instance on a  
4 second lattice domain different from the first symbolic lattice domain.

1 21. A formal verification method comprising:

2 defining an assertion graph including an antecedent label and a  
3 consequence label;

4 simulating a finite state system having an initial state condition or an input  
5 to generate a subsequent state condition or an output;

6 comparing the initial state condition or the input to any antecedent along  
7 an infinite transition path through the assertion graph to identify any  
8 antecedent violation; and

9 comparing the subsequent state condition or the output to the  
10 consequence if no antecedent violation was identified.

1 22. A verification system comprising:

2 means for initializing a symbolic simulation relation for an assertion graph  
3 on a first symbolic lattice domain.

1 23. The verification system of Claim 22 wherein the means for initializing the  
2 symbolic simulation relation comprises:

3 means for joining a Boolean predicate for an outgoing edge from an initial  
4 vertex in the assertion graph with a symbolic antecedent labeling of an edge  
5 in the assertion graph.

1 24. The verification system of Claim 23 wherein the symbolic antecedent labeling  
2 comprises a symbolic indexing function to encode a plurality of antecedent  
3 labels for a plurality of assertion graph instances, having at least one  
4 assertion graph instance on a second lattice domain different from the first  
5 symbolic lattice domain.

- 1 25. The verification system of Claim 22 further comprising:
- 2       means for computing the symbolic simulation relation for the assertion
- 3       graph on the first symbolic lattice domain; and
- 4       means for comparing the symbolic simulation relation to a symbolic
- 5       consequence labeling for the edge for the assertion graph on the first
- 6       symbolic lattice domain.
- 1 26. The method recited in Claim 25 wherein the means for computing the
- 2       symbolic simulation relation comprises:
- 3       means for joining into what is already contained by the symbolic
- 4       simulation relation for the assertion graph on the first symbolic lattice domain,
- 5       any states that are contained by a symbolic antecedent for a first plurality of
- 6       edges of the assertion graph on the first symbolic lattice domain and also
- 7       contained by a symbolic post-image for a second plurality of edges incoming
- 8       to the first plurality of edges.
- 1 27. The verification system of Claim 9 wherein the assertion graph on the first
- 2       symbolic lattice domain is configurable to express a justification property to
- 3       verify through computing the symbolic simulation relation.
- 1 28. The verification system of Claim 27 further comprising:
- 2       means for computing the symbolic simulation relation for the assertion
- 3       graph on the first symbolic lattice domain; and
- 4       means for checking the symbolic simulation relation to verify a plurality of
- 5       properties expressed by a plurality of corresponding assertion graph
- 6       instances, having at least one assertion graph instance on a second lattice
- 7       domain different from the first symbolic lattice domain.
- 1 29. A verification system comprising:
- 2       means for specifying a justification property with an assertion graph.

- 1    30. The verification system of Claim 29 wherein the assertion graph is on a first  
2       symbolic lattice domain; and the justification property is expressed by one of  
3       a plurality of instances of the assertion graph, at least one assertion graph  
4       instance on a second lattice domain different from the first symbolic lattice  
5       domain.

00000000000000000000000000000000